What is Claimed:

1. A method employed on a server computer for switching from a first encryption algorithm to a second encryption algorithm, comprising:

receiving an encryption algorithm negotiation request from a client computer, wherein the encryption algorithm negotiation request specifies an encryption algorithm for subsequent communications between the client computer and the server computer; and

sending a subsession key to the client computer, wherein the subsession key may be used by the client computer in conjunction with the specified encryption algorithm to encrypt future communications to the server computer.

2. A method according to claim 1, wherein the receiving and sending are performed as part of an authentication protocol.

3. A method according to claim 2, wherein the authentication protocol is a Generic Security Services Application Programming Interface ("GSSAPI") implementation of a Kerberos authentication protocol.

4. A method according to claim 3, wherein the encryption algorithm negotiation request is a context negotiation flag in a checksum that is received by the server computer with an Authentication Protocol Request ("AP-REQ").

5. A method according to claim 4, wherein the AP-REQ is encrypted using one of the Ron's Code 4 ("RC4") encryption algorithm, the Data Encryption Standard ("DES") encryption algorithm, and the Triple Data Encryption Standard ("3DES") encryption algorithm.

6. A method according to claim 5, wherein the encryption algorithm negotiation request specifies the Advanced Encryption Standard ("AES") encryption algorithm for subsequent communications between the client computer and the server computer.

7. A method according to claim 1, further comprising determining the encryption algorithm for subsequent communications between the client computer and the server computer by deriving an encryption algorithm from a key sent with said encryption algorithm negotiation request.

8. A computer readable medium containing instructions for a process of negotiating an encryption algorithm between two or more computers, said process comprising:

sending an encryption algorithm negotiation request to a server computer indicating that a client computer supports a specified encryption algorithm; and

anticipating a subsession key from the server computer for use with the specified encryption algorithm; and

switching to the specified encryption algorithm if the subsession key for use with the specified encryption algorithm is delivered.

9. The computer readable medium containing instructions for a process of claim 8, wherein said a process further comprises authenticating the server computer.

10. The computer readable medium containing instructions for a process of claim 9, wherein the authentication protocol is a Generic Security Services Application Programming Interface ("GSSAPI") implementation of a Kerberos authentication protocol.

11. The computer readable medium containing instructions for a process of claim 10, wherein the encryption algorithm negotiation request is a context negotiation flag in a checksum that is received by the server computer with an Authentication Protocol Request ("AP-REQ").

12. The computer readable medium containing instructions for a process of claim 11, wherein the AP-REQ is encrypted using one of the Ron's Code 4 ("RC4") encryption algorithm, the Data Encryption Standard ("DES") encryption algorithm, and the Triple Data Encryption Standard ("3DES") encryption algorithm..

13. The computer readable medium containing instructions for a process of claim 12, wherein the encryption algorithm negotiation request specifies the Advanced Encryption Standard ("AES") encryption algorithm for subsequent communications between the client computer and the server computer.

14. A modulated data signal containing instructions for carrying out the process of negotiating an encryption algorithm between two computers of claim 8.

15. A method for automatically negotiating an encryption algorithm when a first computer requests access to a second computer, comprising:

receiving at the first computer a function call made by an application to an Application Programming Interface("API"); and

initiating in the first computer an authentication protocol process to authenticate the first computer to the second computer; and

including a negotiation request with an authentication protocol process communication from the first computer to the second computer, wherein the negotiation request specifies that the first computer supports one or more encryption algorithms.

16. The method of claim 15, wherein the negotiation request is a key, and wherein a supported encryption algorithm may be derived from the key.

17. The method of claim 15, further comprising anticipating a subsession key from the second computer for use with one or more of said one or more encryption algorithms.

18. The method of claim 17, further comprising switching by the first computer to one of said one or more encryption algorithms upon receiving said subsession key, wherein switching by the first computer is for the purpose of subsequent communications with the second computer.

19. A computer readable medium containing instructions for carrying out the steps of claim 17.

20. A modulated data signal containing instructions for carrying out the steps of claim 17.

21. The method of claim 17, wherein the authentication protocol process to authenticate the first computer to the second computer is a Kerberos authentication protocol process.

22. The method of claim 17, wherein the negotiation request specifies that the first computer supports the AES encryption algorithm.

23. The method of claim 17, wherein the negotiation request is in the form of a context negotiation flag in a checksum generated by a function call to the General Security Services Application Programming Interface ("GSSAPI").

24. A means for negotiating an encryption algorithm between two or more computers involved in an authentication protocol, comprising:

means for reading a negotiation request from a first computer, wherein said negotiation request specifies one or more encryption algorithms supported by the first computer, and wherein the negotiation request is included with an authentication protocol communication from the first computer; and

means for switching to one or more of said one or more encryption algorithms for the purpose of subsequent communications with said first computer.

25. A means for negotiating an encryption algorithm according to claim 24, further comprising means for calculating and delivering a subsession key to the first computer for use with said one or more encryption algorithms.

26. A means for negotiating an encryption algorithm according to claim 25, wherein the negotiation request specifies the Advanced Encryption Standard ("AES") encryption algorithm for subsequent communications between the client computer and the server computer.

27. A means for negotiating an encryption algorithm according to claim 24, wherein the authentication protocol is a Generic Security Services Application Programming Interface ("GSSAPI") implementation of a Kerberos authentication protocol.

28. A means for negotiating an encryption algorithm according to claim 27, wherein the encryption algorithm negotiation request is a context negotiation flag in a checksum that is received by the server computer with an Authentication Protocol Request ("AP-REQ").